Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC. 20554

In the Matter of:	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	

COMMENTS OF U S WEST, INC.

Of Counsel

Dan L. Poole
U S WEST, Inc.

William T. Lake
John H. Harwood II
Samir Jain
Todd Zubler
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, D.C. 20037-1420
(202) 663-6000

Kathryn Marie Krause
Edward M. Chavez
1020 19th Street, N.W.
Washington, DC 20036
(303) 672-2859

Counsel for

U S WEST, INC.

May 20, 1998

SUMMARY

The punch list items demanded by DOJ/FBI are outside the scope of section 103. This is clear from the plain language of the statute and from Congress's direction that CALEA does not (1) require capabilities that go beyond what is permitted under Title III and the ECPA, or (2) allow law enforcement to acquire information that it could not obtain previously. Thus, DOJ/FBI seek to transform CALEA from a limited statute designed to preserve existing capabilities into an all-purpose tool for gathering evidence of every sort.

Even if DOJ/FBI could show that one or more of the punch list capabilities falls within the scope of section 103 (and they have not), the Commission should nonetheless refrain from adding such capabilities to the Interim Standard. Section 107(b) provides that, where an industry standard is challenged in a deficiency petition, the Commission should take account of four important public interest factors in deciding whether to modify the standard. Revising the standard to include the punch list capabilities would be inconsistent with these factors. DOJ/FBI have given short shrift to Congress's concern that carriers and ratepayers not be burdened with unreasonable costs, that privacy and security interests be respected, and that incentives to develop new technology not be dampened.

If the Commission does modify the Interim Standard, it should in no event prescribe that compliance with that standard is the *exclusive* means of satisfying section 103. Compliance with a Commission standard is *one* way — but not the *only* way — of complying with section 103. Furthermore, the Commission should remand any necessary technical standardization work to the appropriate standard-setting organizations and give those bodies the latitude they need to implement the capabilities in an efficient and technically sound manner

Finally, the Commission should confirm that any participation by DOJ or the FBI in a rulemaking must be on the record and comply with the Commission's normal ex parte rules. Section 107(b) does not grant DOJ or the FBI any special role or jurisdiction in determining the deficiency of an industry standard.

TABLE OF CONTENTS

SUMMARY i

BACKGROUND 3

ARGUMENT 11

I. THE COMMISSION SHOULD NOT ADD THE PUNCH LIST ITEMS TO THE INTERIM STANDARD BECAUSE THOSE ITEMS ARE BEYOND THE SCOPE OF WHAT CALEA REQUIRES AND THE COST OF THE ITEMS TO CARRIERS AND RATEPAYERS WOULD BE UNREASONABLE 11

A. The Punch List Capabilities Are outside the Scope of What CALEA Requires Carriers To Provide 12

1. Ability to intercept the communications of all parties in a conference call supported by the subscriber's service or facilities 12

2. Access to call-identifying information 14

a. Subject-initiated dialing and signaling activity 15

b. Information on participants in a multi-party call 17

c. Access to all network-generated in-band and out-of-band signaling 20

3. Delivery of call-identifying information on call data channel and timely delivery of call-identifying information 21

4. Automated delivery of surveillance status information 23

5. Standardization of delivery interface protocols 25

B. Revising the Interim Standard To Include the Punch List Capabilities Would Be Inconsistent with the Public Interest Factors Enumerated in the Statute 25

II. IN NO EVENT SHOULD THE COMMISSION PROPOSE A RULE THAT MAKES ANY PARTICULAR STANDARD THE MANDATORY, EXCLUSIVE MEANS OF COMPLYING WITH SECTION 103 OF CALEA 28

III. IF THE COMMISSION REVISES THE INTERIM STANDARD, IT SHOULD DEFINE ANY NEW CAPABILITIES AT A GENERAL LEVEL AND LEAVE THE DEVELOPMENT OF TECHNICAL REQUIREMENTS TO THE APPROPRIATE STANDARD-SETTING ORGANIZATIONS 31

IV. DOJ/FBI PARTICIPATION IN ANY RULEMAKING SHOULD BE ON THE RECORD AND COMPLY WITH THE COMMISSION'S NORMAL EX PARTE RULES 33

CONCLUSION 34

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC. 20554

In the Matter of:	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	

COMMENTS OF U S WEST, INC.

U S WEST, Inc. ("U S WEST") submits these comments on the deficiency petition filed jointly by the Department of Justice and the Federal Bureau of Investigation ("DOJ/FBI") concerning the capability assistance requirements of section 103 of the Communications Assistance for Law Enforcement Act ("CALEA").[1/] U S WEST urges the Commission to deny the DOJ/FBI deficiency petition in its entirety. As set forth more fully below, in adopting CALEA, Congress established a regime working a limited *quid pro quo*. Carriers are required to have certain limited electronic surveillance capabilities so that law enforcement agencies will continue to have the same access to call content and call-identifying information despite the use of new digital technologies. As FBI Director Louis Freeh repeatedly testified before Congress, all law enforcement sought from CALEA was the ability to maintain the status quo.

In return, carriers are assured of an opportunity to recover their costs of providing those capabilities, and both carriers and the ratepaying public are protected against unreasonable costs. Thus, Congress took care to ensure that law enforcement agencies could not irresponsibly

---

1/ *See* Public Notice (April 20, 1998) (DA 98-762).

"goldplat[e]" their capability requirements.[2/] Furthermore, Congress authorized a specific amount for direct reimbursement of carriers and provided that carriers may seek rate increases from the Commission for unreimbursed costs. In short, Congress envisioned that carriers would provide limited surveillance capabilities in exchange for a limited reimbursement structure.

DOJ/FBI's deficiency petition simply ignores this scheme. It seeks numerous capabilities that would provide access to vast new categories of information and would create capabilities that law enforcement could not lawfully use under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. § 2510-22, or the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. §§ 3121-27. More specifically, DOJ/FBI's capability demands (1) go beyond the plain textual requirements of section 103; (2) violate congressional intent by expanding law enforcement's surveillance capabilities beyond statutory (and even constitutional) bounds; and (3) ignore Congress's direction that CALEA should preserve the electronic surveillance status quo. In short, DOJ/FBI seek to transform CALEA from a limited statute designed to preserve existing capabilities into an all-purpose tool for gathering evidence of every sort. Congress intended none of this.

What is more, even if DOJ/FBI's demands were not wholly ultra vires, as they are, the Commission should nonetheless deny their petition based on the factors set forth is section 107(b) of CALEA. DOJ/FBI have given short shrift to Congress's concern that carriers and ratepayers not be burdened with unreasonable costs, that privacy and security interests be respected, and that incentive to develop new technology not be dampened.

[2/] *See* H.R. Rep. No. 103-827, at 49 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3515 (additional view of Representatives Don Edwards and Rick Broucher) (stating that the Commission should not allow "goldplating" such as "the government asking for upgrades that are unnecessary").

Finally, the Commission should reaffirm that a CALEA standard adopted by either industry or the Commission is only one way for carriers to comply with section 103, rather than the exclusive, mandatory means to comply, as suggested by DOJ/FBI. Moreover, if the Commission decides to modify the Interim Standard in any respect, it should remand the revised standard for implementation by the expert standard-setting organization that has been developing technical requirements for CALEA for over three years.

BACKGROUND

A. *Electronic Surveillance prior to CALEA.* Before Congress enacted CALEA in 1994, federal electronic surveillance was governed primarily by three sources: Title III, the ECPA, and the Fourth Amendment. Each of these authorities restricted law enforcement's ability to conduct electronic surveillance. Title III and the ECPA also defined carriers' obligations to assist law enforcement agencies in carrying out such surveillance and ensured that carriers would be able to recover their costs of providing such service.

1. *Title III.* Title III imposed (and continues to impose) very strict limitations on the ability of law enforcement to obtain call content. Congress adopted Title III after the Supreme Court held in *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967), that the interception of a telephone conversation constitutes a search and seizure under the Fourth Amendment. Congress intended, and the Court has concluded, that Title III's privacy protections would implement the Fourth Amendment's probable cause and particularity requirements. *See Dalia v. United States*, 441 U.S. 238, 256 n.18 (1979); *see also* S. Rep. No. 1097, at 66 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153. And although Title III and the Fourth Amendment are not coextensive in all respects, courts have interpreted the probable cause and particularity requirements of Title III and the Fourth Amendment as being

similar, if not identical. *See, e.g.*, *United States v. Torres*, 751 F.2d 875, 885 (7th Cir. 1984) ("[A] warrant for television surveillance that did not satisfy the four provisions of Title III that implement the Fourth Amendment's requirement of particularity would violate the Fourth Amendment."); *see also United States v. Leisure*, 844 F.2d 1347, 1354 (8th Cir. 1988) ("[T]he statutory probable cause standards set out in Title III are co-extensive with the constitutional requirements embodied in the fourth amendment."). Thus, an interception that satisfies Title III is presumptively valid under the Fourth Amendment, but an interception that violates Title III raises serious constitutional concerns.

Under Title III, law enforcement agencies are prohibited from intercepting wire, oral, and electronic communications unless they obtain a court order or unless exigent circumstances exist.[3/] *See* 18 U.S.C. §§ 2511, 2516, 2518. To obtain such an order, a law enforcement agency must provide a court with a comprehensive application containing (1) details regarding the alleged offense, (2) a particular description of the nature and location of the facilities from which the communication is to be intercepted, (3) a particular description of the type of communications to be intercepted, and (4) the identity of the person, if known, committing the offense and whose communications are to be intercepted. *Id.* § 2518(1)(b). A court may grant the order on finding that (1) there is probable cause to believe a person has committed or is about commit an offense, communications concerning the offense will be obtained from an interception, and the facilities from which the communications are to be intercepted are commonly used by the person or are being used in connection with the offense;

[3/] Under the statute's definitions, ordinary telephone conversations are considered "wire" communications. *See Briggs v. American Air Filter Co.*, 630 F.2d 414, 417 (5th Cir. 1980); *United States v. Harpel*, 493 F.2d 346, 349 (10th Cir. 1974).

and (2) other normal investigative techniques have not succeeded or are unlikely to succeed. *Id.* § 2518(3). The court order must be specific. Among other things, it must specify the *person*, if known, whose communications are to be intercepted and the nature and location of the communications *facilities* as to which interception authority has been granted.

Title III also imposes limited obligations on carriers to assist law enforcement with electronic surveillance: Carriers must furnish a law enforcement agency with "all information, facilities, and technical assistance necessary to accomplish" an interception. 18 U.S.C. § 2518(4). In turn, law enforcement agencies are obligated to compensate carriers for "reasonable expenses incurred in providing such facilities or assistance." *Id.*

2. *ECPA*. Title III's rigorous requirements extend only to the *contents* of communications, not to information *about* communications. *See United States v. New York Tel. Co.*, 434 U.S. 159, 166-68 (1977).[4/] In 1986, however, Congress enacted the ECPA to supplement Title III by providing privacy protection for information *about* communications. Under the ECPA, a law enforcement agency must obtain a court order to use a pen register or trap-and-trace device, *see* 18 U.S.C. § 3121(a), and a court may grant such an order only after the government certifies to the court that the information likely to be obtained is "relevant to an ongoing criminal investigation." *Id.* § 3123(a). The ECPA also requires carriers to provide law enforcement agencies with the information, facilities, and technical assistance necessary to install

---

[4/] The statute limits law enforcement's ability to "intercept" communications, *see* 18 U.S.C. § 2511(1), and the statute defines "intercept" narrowly: "the aural or other acquisition of the *contents* of any wire, electronic, or oral communication." 18 U.S.C. § 2510(4) (emphasis added). "Contents," in turn, is defined under Title III as including "any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

pen registers and trap-and-trace devices, *see* 18 U.S.C. § 3124(a), (b), and carriers are entitled to be "reasonably compensated" for such facilities and assistance, *see id.* § 3124(c).

B. *Origins and Adoption of CALEA.* Although carriers have long met law enforcement's needs by providing service in response to lawful requests under Title III and the ECPA, law enforcement agencies became concerned in the early 1990s that technological developments in telephone services would reduce their ability to use electronic surveillance to obtain the information that they had obtained in the past. Law enforcement was concerned that existing statutes did not clearly obligate carriers to upgrade their capabilities in response to the emerging need law enforcement perceived.[5/]

CALEA grew out of these concerns. But its eventual shape also was heavily influenced by other concerns as well — concerns about the cost to the public fisc and to ratepayers of the new features that law enforcement sought, and about the privacy interests of persons whose call content or call-identifying information law enforcement might obtain. The statute ultimately adopted by Congress represents a careful balance of these different interests and concerns. Of particular relevance here, the statute limits the new capabilities that carriers will be required to provide, *see* 47 U.S.C. § 1002(a), (b); it ensures that carriers will recover their costs of providing those capabilities either from law enforcement or from ratepayers, *see id.* §§ 229(e), 1008; and it ensures that ratepayers will not bear an unreasonable economic burden as a result of law enforcement's demands, *see id.* §§ 1006(b), 1008(b)(1).

5/ *See Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings before the Subcomm. on Tech. and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary on H.R. 4922 and S. 2375*, 103d Cong. 23 (1994) (testimony of FBI Director Freeh) (hereinafter *March Hearing*); *see also* H.R. Rep. No. 103-827, at 13-14, *reprinted in* 1994 U.S.C.C.A.N. at 3493-94.

In addition, Congress intended CALEA merely to *maintain* law enforcement's existing, lawful surveillance capabilities in the face of technological developments. The statute did not give law enforcement carte blanche to require carriers to provide every feature that a law enforcement agency might wish to have. In attempting to persuade Congress to adopt CALEA, DOJ/FBI repeatedly emphasized that CALEA would require carriers to provide only limited additional capabilities to law enforcement agencies. FBI Director Freeh emphasized in both his spoken and prepared testimony to Congress that the FBI's proposal (which was broader that what Congress ultimately adopted) was meant only to "maintain technological capabilities commensurate with existing statutory authority — that is, to prevent advanced telecommunications technology from repealing, de facto, *statutory* authority now existing and conferred to us by Congress." *March Hearing*, *supra*, at 7 (emphasis added); *see also id.* at 6 (stating that the FBI "was not seeking any expansion of the authority Congress gave to law enforcement when the wiretapping law was enacted 25 years ago"). The House Judiciary Committee expressly recognized this principle, stating that the bill "will not expand" law enforcement's statutory authority to conduct electronic surveillance. *See* H.R. Rep. No. 103-827, pt. 1, at 17 (1994), *reprinted in* 1994 U.S.C.C.A.N. at 3497.

In addition to leaving law enforcement's statutory *authority* unchanged, Congress also intended CALEA to preserve the status quo in terms of what information law enforcement could actually acquire through electronic surveillance. Congress, in other words, intended that CALEA would maintain the existing balance that had been struck in electronic surveillance between law enforcement and privacy interests. Director Freeh, for example, testified to Congress that CALEA "ensures a maintenance of the status quo . . . as it relates to the types of information obtainable through pen resister and trap and trace devices." *March Hearing*, *supra*,

at 32; *see also id.* at 40 ("Under the proposed legislation, law enforcement would acquire this dialing information *as it does today — no more no less.*"). And the House Judiciary Committee relied on this testimony when it approved CALEA. The Committee's report highlights Director Freeh's assurance that law enforcement would receive "no more and no less access to information than it had in the past." H.R. Rep. 103-827, at 22, *reprinted in* 1994 U.S.C.C.A.N. at 3502. Moreover, the Committee specifically stated that "[t]he Committee expects industry, law enforcement and the FCC to narrowly interpret" CALEA's assistance requirements. *Id.* at 23, *reprinted in* 1994 U.S.C.C.A.N. at 3503.

Thus, CALEA requires carriers to provide, not "anything law enforcement asks for," but only four general capabilities.[6/] Under section 103, carriers must ensure that their facilities can

(1) expeditiously isolate and enable the government to intercept a subscriber's wire and electronic communications;

(2) expeditiously isolate and enable the government to access call-identifying information that is reasonably available to the carriers;

(3) deliver intercepted communications and call-identifying information to the government through equipment, facilities, and services procured by the government; and

(4) facilitate these interceptions unobtrusively and in a manner that protects the privacy of other communications.

[6/] The fact that CALEA limits the obligations of carriers does not mean, however, that law enforcement is necessarily precluded from obtaining additional electronic surveillance features from carriers. If those additional capabilities are consistent with Title III, the ECPA, and the Constitution, law enforcement can purchase those features from carriers outside of the CALEA cost-reimbursement context.

See 47 U.S.C. § 1002(a). The act defines "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber." *Id.* § 1001(2).

In addition to setting an outer limit on such capabilities, CALEA also authorizes the Commission, through a variety of mechanisms, to narrow even further what carriers must provide if the cost of providing particular capabilities would be excessive. This authority is intended to protect not only carriers but also ratepayers, who would be affected by any rate increases that carriers seek to cover the costs of CALEA compliance. Such rate increases are specifically authorized under CALEA, *see* 47 U.S.C. § 229(e), and almost certainly will be necessary, especially if carriers are required to implement any of the additional capabilities demanded by DOJ/FBI in their deficiency petition. Congress has authorized only $500 million for the nationwide implementation of CALEA, *see id.* § 1009, while estimates of the total cost of CALEA compliance have ranged into the billions of dollars. *See, e.g.*, *March Hearing*, *supra*, at 14, 164.

Thus, in considering whether to adopt a revised standard under section 107(b), the Commission must consider, among other things, whether the standard "meet[s] the assistance capability requirements of section 103 *by cost-effective methods*" and "*minimize[s] the cost* of such compliance on residential ratepayers." 47 U.S.C. § 1006(b)(1), (3) (emphases added). Similarly, the Commission may relieve carriers of their compliance obligation where such compliance is not "*reasonably* achievable" for certain equipment. *See id.* § 1008(b) (emphasis added). In applying this test, the Commission must consider the effect of compliance on rates for basic residential telephone service, the need to achieve CALEA's requirements "by cost-effective methods," and the financial resources of carriers. *See id.* § 1008(b)(1)(B), (D), (H).

3. *Development of a CALEA Industry Standard.* Law enforcement, carriers, and manufacturers have participated in a consultative process to implement CALEA for more than three years since the statute's enactment. Starting in early 1995, manufacturers and carriers began to develop an "industry" standard to meet the four general capability requirements for carriers. Under section 107(a) of CALEA, compliance with such a standard provides carriers with a safe harbor from enforcement actions. *See id.* § 1006(a).

Manufacturers and carriers worked to develop a safe harbor standard through two standard-setting committees: Subcommittee TR45.2 (sponsored by the Telecommunications Industry Association (TIA)) and Committee T1 (sponsored by the Alliance for Telecommunications Industry Solutions (ATIS)). Both of these bodies are standard-setting organizations accredited by the American National Standards Institute (ANSI).[7/] The committees made substantial progress developing a standard until the second quarter of 1996, when the FBI began to circulate its Electronic Surveillance Interface (ESI) document.[8/] That document set forth the FBI's position on what capabilities are required by CALEA (including certain "punch list" items) as well as detailed technical provisions on *how* those capabilities must, in the FBI's view, be provided.

The committees incorporated most of the ESI features into their draft standard.[9/] Manufacturers, carriers, and law enforcement were thus able to agree on the contents of a

---

7/ *See* Responsive Statement of TIA to the Appeal of the Federal Bureau of Investigation to the Executive Standards Council of the American National Standards Institute, June 19, 1997, at 2.

8/ *See* Petition for Rulemaking, filed by Cellular Telecommunications Industry Association ("CTIA"), July 16, 1997, at 8-9 ("CTIA Petition").

9/ *See id.*

standard that, even in the FBI's view, would fulfill a large portion of section 103's requirements. Although TIA and Committee T1 did not include the punch list items in the Interim Standard/Trial Use Standard J-STD-025 ("Interim Standard")[10/] that they published in December 1997, the committees have continued to cooperate with law enforcement by commencing discussions on an Enhanced Surveillance Services ("ESS") standard that would implement the disputed capabilities.[11/] Nevertheless, on March 27, 1998, DOJ/FBI filed a petition with the Commission contending that the Interim Standard is deficient.[12/]

ARGUMENT

I. THE COMMISSION SHOULD NOT ADD THE PUNCH LIST ITEMS TO THE INTERIM STANDARD BECAUSE THOSE ITEMS ARE BEYOND THE SCOPE OF WHAT CALEA REQUIRES AND THE COST OF THE ITEMS TO CARRIERS AND RATEPAYERS WOULD BE UNREASONABLE.

To prevail on its deficiency petition with respect to any one of the punch list capabilities, DOJ/FBI must show, at a minimum, that the capability falls within the scope of section 103 of CALEA. DOJ/FBI have failed utterly to carry that burden. As we show below, the punch list items demanded by DOJ/FBI are outside the scope of section 103. This is clear

---

10/ *See* TIA Press Release, "TIA and ATIS Publish Lawfully Authorized Electronic Surveillance Industry Standard," December 5, 1997.

11/ *See* TIA Petition at 12 n.18; *see also* Response to Petition for Rulemaking, filed by CTIA, Personal Communications Industry Association ("PCIA"), and United States Telephone Association ("USTA"), April 9, 1998, at 7-9 ("CTIA Response"). Subcommittee TR45.2 is coordinating this standard-setting project, and U S WEST and other carriers have taken part in the discussions.

12/ *See* Joint Petition for Expedited Rulemaking, filed by DOJ and FBI, March 27, 1998, at 1-2 ("DOJ/FBI Petition"). In addition, on March 26, 1998, the Center for Democracy and Technology ("CDT") filed such a petition, asserting that the Interim Standard includes two capabilities not required by CALEA. *See* Petition for Rulemaking under Sections 107 and 109 of the Communications Assistance for Law Enforcement Act, filed by CDT, March 26, 1998.

from the plain language of the statute and from Congress's direction that CALEA does not (1) require capabilities that go beyond what is permitted under Title III and the ECPA, or (2) allow law enforcement to acquire information that it could not obtain previously.

Even if DOJ/FBI could show that one or more of the punch list capabilities falls within the scope of section 103 (ant they have not), the Commission should nonetheless refrain from adding such capabilities to the Interim Standard. Section 107(b) provides that, where an industry standard is challenged in a deficiency petition, the Commission should take account of four public interest factors in deciding whether to modify the standard. Revising the standard to include the punch list capabilities would be inconsistent with these factors.

A. The Punch List Capabilities Are outside the Scope of What CALEA Requires Carriers To Provide.

In support of their deficiency petition, DOJ/FBI rely heavily on their assertion that law enforcement agencies *need* the punch list capabilities. But such needs do not determine the fundamental legal question under CALEA. Section 103 defines the assistance capability requirements in terms of substantive criteria, and those criteria do not encompass the punch list items. Indeed, even though DOJ/FBI have long claimed to have done a comprehensive analysis of the issues, their deficiency petition fails to come to grips with the limits imposed by section 103. DOJ/FBI have not, therefore, provided an adequate basis for the Commission to propose, much less adopt, the punch list capabilities as part of the safe harbor standard.

1. Ability to intercept the communications of all parties in a conference call supported by the subscriber's service or facilities (pp. 27-33)

DOJ/FBI's leading demand is that carriers provide a capability to monitor conversations of parties to a conference call even if the person named in a Title III court order

("intercept subject") has left the call either temporarily or permanently. *See* DOJ/FBI Petition at 27-33. DOJ/FBI contend that this capability is required by CALEA, but they overlook both the limiting effects of Title III and the fact that such a capability would enable law enforcement to expand the reach of its information gathering far beyond the pre-CALEA regime.

DOJ/FBI argue that law enforcement should be permitted to intercept the conversations of persons left on hold because those persons would use the intercept subject's "service" to converse. *See* DOJ/FBI Petition at 27-29. DOJ/FBI point to section 103 of CALEA, which requires carriers to provide the government with the ability to intercept communications to or from the "equipment, facilities, or *services* of a subscriber." 47 U.S.C. § 1002(a)(1) (emphasis added). But section 103 must be read in light of Title III, which requires court orders to specify "the communication *facilities* as to which . . . authority to intercept is granted." 18 U.S.C. § 2518(4)(b) (emphasis added). A conversation among parties after an intercept subject has left a call would be transmitted without any contact with the intercept subject's own facilities. An interception of that conversation would therefore be beyond the authorization of a Title III court order.[13/] As a result, it would raise serious constitutional concerns. *See* pp. 3-4, *supra*. The Commission should of course avoid construing CALEA in a manner that would present such

---

13/ Nor would the portion of Title III relating to "roving" wiretaps provide a lawful basis for such an interception. *See* 18 U.S.C. § 2518(11)(b). Although this provision gives law enforcement more flexibility with respect to *facilities* under certain circumstances, it exacts a *quid pro quo* — requiring court orders to identify the *specific person* whose conversations will be intercepted. *Id.* § 2518(11)(b)(ii). Indeed, courts have upheld roving wiretaps as constitutional precisely because Title III requires such wiretaps to be person-specific. *See, e.g.*, *United States v. Bianco*, 998 F.2d 1112, 1124 (2d Cir. 1993); *United States v. Petti*, 973 F.2d 1441, 1445 & n.3 (9th Cir. 1992). The capability demanded by DOJ/FBI would intercept communications from facilities that were never specified in a court order and of persons that were never identified as intercept subjects. DOJ/FBI, in other words, would avoid the obligation to specify facilities *and* the obligation to specify the person. This they may not do.

issues. *See Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988); *Weaver v. United States Info. Agency*, 87 F.3d 1429, 1436 (D.C. Cir. 1996), *cert. denied*, 117 S. Ct. 2407 (1997).

Finally, even if this capability did not offend Title III, the DOJ/FBI proposal would do much more than *maintain* law enforcement's actual surveillance capabilities in the face of new digital telephony technology. Rather, it would clearly *expand* them. As even DOJ and the FBI acknowledge, "Congress made clear that its intent in imposing assistance requirements on telecommunications carriers was 'to preserve the status quo'." DOJ/FBI Petition at 16 (quoting H.R. Rep. No. 103-827, at 22, *reprinted in* 1994 U.S.C.C.A.N. at 3502). Yet conference calls existed long before any recent technological innovations in telephony, and law enforcement agencies have not previously been able to intercept conversations after an intercept subject has left such a call. DOJ/FBI seek a capability, for the first time, to intercept a person's private conversations merely because the person had previously been on a conference call with an intercept subject. Congress did not intend that result.

2. Access to call-identifying information (pp. 33-47)

The DOJ/FBI petition also argues for three related capabilities that supposedly provide "call-identifying information." Section 103(a)(2) of CALEA requires a carrier to enable law enforcement to "access call-identifying information that is reasonably available to the carrier." 47 U.S.C. § 1002(a)(2). To be required by CALEA, therefore, a capability must pass two tests: (1) it must provide "call-identifying information" as defined by CALEA, and (2) the call-identifying information must be "reasonably available" to carriers.

On the second of these questions, the DOJ/FBI petition is silent. It simply does not address the technical and cost issues that would be relevant to whether the information

involved is reasonably available. Without any such showing by DOJ/FBI, the Commission should be hesitant to upset a standard that was carefully developed by experts at accredited standard-setting organizations. On the first question — whether the requested capabilities even provide call-identifying information — the DOJ/FBI petition advances positions that have no merit.

a. Subject-initiated dialing and signaling activity (pp. 36-42)

DOJ/FBI argue that carriers must provide law enforcement with "subject-initiated dialing and signaling activity." DOJ/FBI includes within this category so-called "post-cut-through digits."[14/] These are numbers dialed by a subscriber after a call initially goes through to its terminating destination (*i.e.*, after the call "cuts through"). Calling and prepaid cards, for example, typically require a caller first to dial an 800 number and then, after connecting to an interexchange carrier ("IXC"), to dial a second telephone number. The second number comprises post-cut-through digits. DOJ/FBI propose to require carriers to ensure that their facilities can extract "the digits dialed by the subject following cut-through." *See* DOJ/FBI Petition, Appendix 1, at 16-17.

This capability plainly goes beyond "call-identifying information." CALEA defines that term as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber." 47 U.S.C. § 1001(2). For a local exchange carrier ("LEC"), that definition refers to the dialing and

---

[14/] DOJ/FBI also address the use of flash hooks and feature keys during a telephone call under the heading "subject-initiated dialing and signaling activity." *See* DOJ/FBI Petition at 36-38. Because this information is similar to that provided by the capability discussed in subsection "b" below, we address those issues together there.

signaling information used to connect the caller *to the IXC*; as far as the LEC is concerned, that information "identifies the . . . direction, destination [and] termination" of the call. Once the intercept subject establishes a connection with the IXC, the direction, destination, and termination of the call are fixed. The call has terminated at the IXC's platform. The LEC has no special access to or reason to know the second number.[15/] Law enforcement may *want* the LEC to provide both the 800 number and the second number, but Congress made clear that CALEA "is not intended to guarantee 'one-stop shopping' for law enforcement." H.R. Rep. No. 103-827, at 22, *reprinted in* 1994 U.S.C.C.A.N. at 3502. Indeed, the House report states that, if an advanced intelligent network directs a communication "to a different carrier, the subscriber's carrier only has the responsibility . . . to ensure that law enforcement can identify the new service provider handling the communication." *Id.*

Moreover, many post-cut-through digits will be entirely unrelated to the origin, direction, destination, or termination of a communication. A person who conducts electronic banking over the phone, for example, will dial many post-cut-through digits that will not identify the communication in any way. FBI Director Freeh told Congress that the FBI wanted access only to "telephone numbers which are being called," not to transactional data such as numbers

---

15/ DOJ/FBI attempt to support their position by citing a Commission statement that a calling card call is not "completed" until is answered by the called party. DOJ/FBI Petition at 41 (citing *Implementation of the Pay Telephone Reclassification and Compensation Provisions of the Telecommunications Act of 1996*, CC Docket No. 96-128, Report and Order, 11 FCC Rcd. 20541, 20573 ¶ 63 (1996) ("*Pay Telephone Order*")). That statement, however, is taken from a Commission order that is entirely unrelated to CALEA and, indeed, unrelated to electronic surveillance generally. In fact, the order's preceding sentence states that the Commission was determining "what constitutes a 'completed call' *for purposes of per-call compensation*." *Pay Telephone Order*, 11 FCC Rcd. at 20574 ¶ 63. The Commission therefore made its determination based on a variety of economic and consumer issues that bear no relation to the statutory and technical feasibility issues relevant to CALEA.

dialed for banking purposes. *March Hearing*, *supra*, at 50. According to Director Freeh, "I do not want it, do not need it, and I am willing to have technological blocks with respect to that information." *Id.* Indeed, CALEA expressly amended the ECPA to limit pen registers to the recording of "the dialing and signaling information *utilized in call processing*." 18 U.S.C. § 3121(c) (emphasis added). But the DOJ/FBI proposal would require carriers to provide *transactional* data that have nothing to do with *call processing*. The proposal therefore would require carriers to provide information beyond the scope of the ECPA and thus outside CALEA's definition of call-identifying information.

Furthermore, the fact that law enforcement may have been able to access all post-cut-through digits in the past does not support the DOJ/FBI proposal.[16/] As noted above, at the same time it enacted CALEA, Congress amended the ECPA to *limit* the use of pen registers to the collection of "information utilized in call processing." 18 U.S.C. § 3121(c). Thus, regardless of what information law enforcement was able to acquire with pen registers prior to CALEA, Congress expressly narrowed law enforcement's authority in 1994. In this limited context, therefore, Congress did not intend to preserve the status quo. The Commission should accordingly reject the DOJ/FBI proposal, which would provide law enforcement with far more than "information utilized in call processing."

b. Information on participants in a multi-party call (pp. 42-45)

DOJ/FBI next argue that CALEA call-identifying information provisions require carriers to provide detailed information to law enforcement about who is a party to a call at any given time. They propose, for example, that carriers provide messages indicating when any party

---

16/ *See* DOJ/FBI Petition at 39 & n.17.

is joined, dropped, or put on hold during a conference call involving the intercept subject. *See* DOJ/FBI Petition at 42-45. In addition, the DOJ/FBI petition demands that carriers provide law enforcement with information about an intercept subject's use of feature keys and flash hooks to manipulate a call. *See id.* at 36-38. DOJ/FBI attempt to justify these closely related capabilities by claiming that law enforcement needs to know who is speaking with whom at any point during a telephone call for investigatory and evidentiary purposes. *See id.* at 37, 43. But DOJ/FBI fail to show that CALEA requires these capabilities, and they even admit that the capabilities go beyond the electronic surveillance status quo.

First, although conference calling, feature keys, and flash hooks allow parties to conduct more complex telephone communications, law enforcement agencies do not need the demanded capabilities to obtain the dialing information traditionally available through pen registers and trap-and-trace devices. Even without the punch list capabilities, law enforcement agencies will be able to acquire the telephone numbers that an intercept subject dials and the telephone numbers of persons who call the intercept subject, regardless of whether the intercept subject uses conference calls or feature keys. Thus, DOJ/FBI are demanding new information: They want to be able to track the *course* of every conversation by knowing "to whom the subject is speaking at any point in the conversation."[17/]

Nothing in section 103 requires carriers to provide such information. CALEA defines call-identifying information as "dialing or signaling information that identifies the *origin, direction, destination, or termination* of each communication generated or received by a subscriber." 47 U.S.C. § 1001(2) (emphasis added). Information about how a subscriber moves

---

17/ DOJ/FBI Petition at 37.

back and forth between calls does not fall within this definition. Once an intercept subject establishes a line of communications with another party, the origin, direction, destination, and termination of that communication are fixed. If the intercept subject puts the party on hold or adds another party, neither action alters the "origin, direction, destination, and termination" of the original communication.

In addition to falling outside CALEA's definition of "call-identifying information," these capabilities exceed law enforcement's statutory authority under the ECPA. The ECPA defines pen registers and trap-and-trace devices narrowly, permitting law enforcement to record only impulses that identify telephone numbers. *See* 18 U.S.C. § 3127(3), (4). Information about who is participating on a conference call does not fall within the ECPA definitions. And these capabilities therefore would raise constitutional issues as well, which the Commission should avoid.[18/]

Finally, even DOJ/FBI admit that law enforcement has never been able "to obtain information that a particular participant was placed on hold during, or dropped from, a multi-party call, because such information resided within, and required access to, the switch." DOJ/FBI Petition at 44. Indeed, law enforcement could identify only "the range of participants

---

18/ In contrast to Title III, the ECPA was not intended to comply with any particular decision by the Supreme Court. The Court's only substantial analysis of how the Fourth Amendment applies to information *about* communications was in *Smith v. Maryland*, 442 U.S. 735 (1979), where the Court held that the use of pen registers did not implicate the Fourth Amendment. *Smith*'s holding, however, was quite narrow. The Court assumed that pen registers record only the telephone number dialed and no other information about a communication. *Id.* at 741. Indeed, the Court assumed that pen registers would not even indicate whether a call was completed. *Id.* And the Court noted that telephone users have no legitimate expectation of privacy in numbers they dial because telephone companies typically record such numbers in the ordinary course of business. *Id.* at 742-44. These narrow assumptions suggest that the Court might give stronger constitutional protection to communication attributes that reveal more private information.

who might be involved in a multi-party call" and would have to "infer specifically which participants heard portions of the call." *Id.* But this fact gives DOJ/FBI no pause. In the very next sentence of their petition, they assert that CALEA "now obligates carriers to provide this information." *Id.* DOJ/FBI thus ignore Director Freeh's assurances to Congress that law enforcement would acquire call-identifying information under CALEA "*as it does today—no more no less*." *March Hearing*, *supra*, at 40.

c. Access to all network-generated in-band and out-of-band signaling (pp. 45-47)

DOJ/FBI also demand access, under the rubric "call-identifying information," to in-band and out-of-band signaling sent over carriers' networks. DOJ/FBI apparently seek (1) signals that reveal the result of an intercept subject's call attempt (*e.g.*, whether the line was busy), and (2) signals and messages sent to an intercept subject's phone when a party tries to call the intercept subject. DOJ/FBI, however, never present a clear explanation of why the Interim Standard is deficient in this respect, and they fail to define precisely how the DOJ/FBI proposal would remedy the deficiency. For that reason alone, the Commission should reject DOJ/FBI's request for this capability.

In any event, CALEA plainly does not require the provision of this information. DOJ/FBI attempt to justify their need for signals showing call attempts, for example, by claiming that it identifies the "termination" of a communication. As noted above, however, the "termination" of a communication (as used in the definition of call-identifying information) refers only to the telephone number to which a calling party is connected as a result of dialing an